UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/672,184	09/25/2003	Eduard K. de Jong	SUN-040027	9837

24209 7590 11/26/2007

GUNNISON MCKAY & HODGSON, LLP
1900 GARDEN ROAD
SUITE 220
MONTEREY, CA 93940

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
11/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/672,184	DE JONG, EDUARD K.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) *5,10,15 and 20* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-9,11-14 and 16-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 September 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-4, 6-9, 11-14, and 16-19 were examined. Claims 1, 6, 11, and 16 were amended, which changed the scope of the claims from what was previously presented. Any new rejections made in this office action were necessitated by the amendments.

This application contains claims 5, 10, 15, and 20 which are drawn to an invention nonelected with traverse in the reply filed on 9/18/07. A complete reply to the final rejection must include cancellation of nonelected claims or other appropriate action (37 CFR 1.144) See MPEP § 821.01.

Information Disclosure Statement

The documents listed in the IDS submitted on 9/4/07 were considered.

Drawings

The drawings were received on 9/18/07. These drawings are acceptable.

Response to Arguments

With respect to the restriction requirements previously made FINAL, applicant presented further arguments that a proper restriction was not made. Applicant states that the examiner's previous argument that the MPEP does not present any guidelines towards just process of making and using is incorrect. Applicant cited MPEP 806.05 to support applicant's arguments. The examiner respectfully notes that the portion cited by applicant deals with restriction by combination and subcombination and subcombinations disclosed as usable together. The examiner had restricted the claims as subcombinations disclosed as usable together, thus it would appear that the portion cited by applicant only serves to strengthen the examiner's position rather than

applicant's since applicant had previously argued that if a restriction was to be made, it should have been made as process of making and process of using rather than as subcombinations disclosed as usable together. The invention of group I (claims 1-4, 6-9, 11-14, and 16-20) contain limitations not found in group II (claims 5, 10, 15, and 20) and vice versa, thus the inventions are two way distinct. Because the two groups contain limitations not found in the other group, it would be a burden to plan and search for two distinct inventions. Contrary to applicant's arguments, applicant's previous arguments were not summarily dismissed as incorrect without consideration. A consideration of the file history will show that applicant's arguments were fully considered, but were found to be incorrect and in fact the portions of the MPEP which applicant has now cited to support applicant's arguments instead support the examiner's position that the claims were correctly restricted as subcombinations disclosed as usable together. The restriction requirement remains FINAL.

With respect to the previously made 101 rejections, applicant argued that the examiner ignored explicit claim limitations in stating that the claims were directed towards software per se. Applicant cites, among other paragraphs from the specification, paragraph 15, as proof that the "means for" language had proper structural support in the specification, thus should not be viewed as software per se. The examiner respectfully disagrees. The portions cited by applicant contain general statements that in one embodiment of the invention, components of the invention could be implemented via firmware, hardware, software, etc., but it was not clear if every component could be implement in the manner disclosed in the paragraphs cited or just

certain components. Further, it was not clear that the "means for" language used in the claims referred to the embodiment of the invention cited by applicant in the latest arguments submitted, especially since the last paragraph of applicant's specification stated that the invention is to be restricted only by the claims. Further, paragraph 15 that was cited by applicant clearly states that components of the invention may be implemented by application programs, thus it would not have been incorrect to interpret the various means recited in the claims as referring to software per se. As applicant recognizes (as evident from applicant's remarks), software by itself cannot accomplish anything, thus applicant in essence admits that applicant's claims which were previously rejected under 35 USC 101 do not do anything since they were directed towards software per se, and as such do not produce any result. Regardless, the previous 101 rejections to claims 11-19 are now withdrawn due to applicant's amendments.

With respect to the 103 rejections, applicant statues that claim interpretation must be limited in that the interpretation must be consisted with the specification. The examiner respectfully submits that this is incorrect. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Further, as previously pointed out, the last paragraph of applicant's specification even instructs that determination of what applicant's claimed invention is should only be limited by the claims.

Applicant argues on page 32 of the remarks filed that the specification provided a definition of "target ID". However, no such explicit definition was found in the

specification. Examples of what "target ID" could be in certain embodiments of applicant's invention is not an explicit definition.

Applicant argues that with respect to claims 1, 6, 11, and 16, Kessler does not disclose obfuscating the encrypted key. However, it is respectfully noted that these claims do not contain any limitations about obfuscating the encrypted key. It is noted that the next to last limitation in claim 1, for example, recites that an encrypted second key is scrambled into said instruction stream using a code obfuscation method to create an obfuscated key decryption program. However, the limitation appears to require that the instruction stream be obfuscated, not the encrypted second key. Just because the encrypted second key was used as an input into an obfuscation method does not mean that it was the key that was obfuscated.

Applicant argues Kessler does not disclose an instruction stream for a key decryption program configured to the decryption algorithm for the first cryptographic key. However, it should be understood that all computer programs are composed of instruction streams. Kessler disclosed of a proprietary client software received by each registered client computer which contains decryption algorithms and keys necessary to decrypt content for use on the client computer (col 8, lines 50-67). There being a program having decryption algorithm implies that there is an instruction stream for a key decryption program configured to the decryption algorithm for the first cryptographic key.

Applicant argues on pages 32-33 of the remarks filed that Kessler taught away from obfuscation of the encrypted key. The examiner respectfully disagrees. First, as

noted already, the claims as recited do not appear to require obfuscation of the encrypted key. Also, column 8, lines 50-67 clearly refer to obfuscation and encryption of the keys themselves within the proprietary client software—the software used to decrypt content.

Applicant's remaining remarks were also fully considered, but are moot due to applicant's amendments and due to new rejections made below in response to the amendments.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Note that with respect to the current application, a person of ordinary skill in the art at the time applicant's invention was made is determined to be someone having at least a BS in Computer Science or Engineering and has experience with software development and various software protection schemes (or someone with equivalent industry experience).

Claims 1-4, 6-9, 11-14, and 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler et al (US 7,170,999) in view of Okada (US 6,789,177) in

further view of Shen Orr (WO 02/079955) in further view of LeVine et al (US 2002/0120854).

As per claim 1, Kessler discloses receiving a reference to a decryption algorithm and a first cryptographic key and creating a key decryption program (i.e. proprietary client software having embedded decryption algorithms) comprising an instruction stream, said key decryption program configured to perform said decryption algorithm for said first cryptographic key (col 8, lines 50-67 and col 10, lines 58-67). *A person skilled in the art should understand that all programs start out as source code and when the source code is compiled, the resulting software contains instruction streams. The cited portion of Kessler discloses of a proprietary client software received by the client. The proprietary software contains decryption algorithms used to access the encrypted data files via keys SK2 and TK. The fact that the proprietary software exists implies that a reference to a decryption algorithm (i.e. decryption algorithm source code) was received and used to create the proprietary software. According to the cited portion in column 8, the keys used in the decryption algorithm are obfuscated and/or encrypted in the proprietary software. This implies that when the proprietary software was created, not only was the source code to the decryption algorithm received, but also the first decryption key, i.e. SK2, which is used to decrypt TK.*

Kessler discloses applying a cryptographic process to a second cryptographic key, i.e. TK, to create an encrypted second cryptographic key wherein said cryptographic process receives a public key and second cryptographic keys as inputs

(col 5, lines 29-42). *Note that TK is encrypted using PK2, which implies that both TK and PK2 were inputs to a cryptographic process.*

Kessler discloses sending said key decryption program (col 4, lines 44-46 and col 8, lines 50-51).

It is noted that in Kessler's invention, a public key PK2 is used to encrypt the second cryptographic key, i.e. TK, while a secret key SK2 is used to decrypt the second cryptographic key. In the invention recited in claim 1, a first cryptographic key is used to both create the encrypted second key and to decrypt the second key, i.e. perform said decryption algorithm for said first cryptographic key. However, Okada discloses using a first cryptographic key, i.e. session key, to both encrypt and decrypt a second key, i.e. content key (col 9, lines 21-26 and col 10, lines 39-53). Note that the content key disclosed by Okada is equivalent to the track key (TK) disclosed by Kessler.

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Kessler's invention such that rather than use an asymmetric key system to encrypt/decrypt the second cryptographic key TK, a symmetric key system was utilized such that a first cryptographic key was used to both encrypt and decrypt the second cryptographic key as per Okada's teachings. One skilled would have been motivated to do so because symmetric key systems are faster and less computationally intensive than asymmetric key systems. Another rationale for why it would have been obvious to modify Kessler's invention in the manner discussed using Okada's teachings is that the simple substitution of Okada's key encrypting key methodology within Kessler's invention would do no more than yield the predictable

result of a track key (TK) being encrypted and decrypted using a single first cryptographic key rather than use of an asymmetric key pair to encrypt and decrypt TK.

Kessler also does not explicitly disclose scrambling, said encrypted second cryptographic key into said instruction stream using a code obfuscation method indicated by an obfuscation descriptor, said scrambling creating an obfuscated key decryption program, said obfuscation descriptor based at least in part on a target ID wherein said target ID specifies a user device for executing an obfuscated application program. Kessler does not disclose the key decryption program that was sent is obfuscated. Kessler does not explicitly disclose the receiving, creating, applying, scrambling, and sending step were all done on the same application program provider.

However, Shen Orr discloses creating an obfuscated key decryption program (p16, line 31-p17, line 3; p21, lines 1-2; and p24, lines 17-19) via use of an obfuscation method indicated by an obfuscation descriptor (p9, lines 19-24 and p9, line 33-p10, line 2), said obfuscation descriptor based at least in part on a target ID wherein said target ID specifies a user device for executing an obfuscated application program (p9, line 33-p10, line 2). *Note that in the cited portions of Shen Orr, several techniques are used to secure a key decryption program, including use of one or more obfuscation methods to render the decryption program obfuscated. The obfuscation method is chosen based on at least one variable parameter which is partially determined by the hardware or software identifier of the end user device—i.e. the target ID.*

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify Kessler's invention using Shen Orr's teachings

by obfuscating Kessler's proprietary client software before sending it to the client via an obfuscation method indicated by an obfuscation descriptor that is based at least in part on a target ID (i.e. the end user's device's hardware or software identifier) that specifies a user device for executing an obfuscated proprietary client software. One skilled would have been motivated to do so because as recognized by Shenn Orr, there was a need in the art to provide variable security mechanisms (p6, lines 20-26), which would provide more security than using a single security scheme such as the one used by Kessler.

Shenn Orr also does not disclose that the obfuscation method involves scrambling said encrypted second cryptographic key into said instruction stream. However, LeVine discloses of an obfuscation method which involves scrambling an encrypted key into the instruction stream of a program (paragraphs 12, 21, 23, 26 and 78).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Kessler's invention such that the obfuscation method used involves scrambling said encrypted second cryptographic key into said instruction stream. The rationale for why it is obvious is that as per Shen Orr's teachings, obfuscation to secure a program was already used in Kessler's modified invention and the substitution LeVine's obfuscation method in place of one of the obfuscation methods used by Shen Orr would do no more than yield the predictable result of obfuscation as per LeVine's methodology.

As per the limitation that the receiving, creating, applying, scrambling, and sending step were all done on the same application program provider, note that in Shenn Orr invention, all the steps of creating an application program to be sent to an end user is performed on a single application builder 102 (Fig 1 and Fig 4A-4B). At the time applicant's invention was made it would have been obvious to one of ordinary skill in the art to have the combination invention of Kessler, Okada, Shen Orr, and LeVine perform all the steps of application program obfuscation on a single application program provider, i.e. application builder. One skilled would have been motivated to do so because it would lessen the chances that someone would obtain the key decryption program before it was secured using Kessler's modified invention.

Claims 6, 11, and 16 recite similar limitations as what is recited in claim 1 and are rejected for similar reasons. Note that Kessler, Okada, Shen Orr, and LeVine's inventions are all performed using computers. All computers contain a processor and a memory, coupled to the processor, having stored therein computer readable instructions that are executed by the processor to perform a method according to the instructions.

Claims 2, 7, 12, and 17:

Kessler further discloses method, medium, means, and apparatus for sending digital content protected by said second cryptographic key (Fig 2 and col 10, lines 58-67).

Claims 3, 8, 13, and 18:

As per claims 3, 8, 13, and 18, Shen Orr further discloses sending said obfuscated key decryption program together with said digital content (p19, line 32-p20, line 8).

Claims 4, 9, 14, and 19:

As per claims 4, 9, 14, and 19, Kessler does not explicitly disclose wherein said target ID comprises a VM ID. However, Shen Orr discloses target ID icluding a software identifier (p10, lines 1-2). Further, official notice is taken that virtual machines having VM ID were well known in the art at the time applicant's invention was made. At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to have the target ID comprise VM ID. One skilled would have been motivated to do so because as disclosed by Shen Orr, software ID could be utilized as a target ID and because virtual machines were known types of software, using the VM ID as a target ID would do no more than yield a predictable result of using a specific type of software ID as the target ID.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100